

p -quotients of the G.Higman group

L. Glebsky

April 22, 2016

Abstract

These notes are based on the mini-course “On the Graham Higman group”, given at the Erwin Schrödinger Institute in Vienna, January 20, 22, 27 and 29, 2016, as a part of the Measured Group Theory program.¹ The main purpose is to describe p -quotients of the Higman group $H(k)$ for $p|(k-1)$. (One may check that the condition $p|(k-1)$ is necessary for the existence of such quotients.)

1 Higman group

Consider the Higman group $H(k) = \langle a_0, \dots, a_3 \mid \{a_i^{-1}a_{i+1}a_i = a_{i+1}^k, i = 0, \dots, 3\} \rangle$, $i+1$ is taking mod 4 here. It may be constructed as successive amalgamated free products, starting from Baumslag-Solitar group $BS(1,k) = \langle a_0, a_1 \mid a_0^{-1}a_1a_0 = a_1^k \rangle$:

$$B_3\langle a_0, a_1, a_2 \rangle = \langle a_0, a_1 \mid a_0^{-1}a_1a_0 = a_1^k \rangle_{a_1 \leftrightarrow a_1} * \langle a_1, a_2 \mid a_1^{-1}a_2a_1 = a_2^k \rangle.$$

Similarly, one may construct $B_3\langle a_2, a_3, a_0 \rangle$ and

$$H_k = B_3\langle a_0, a_1, a_2 \rangle_{a_0 \leftrightarrow a_0, a_2 \leftrightarrow a_2} * B_3\langle a_2, a_3, a_0 \rangle$$

The group $H(2)$ was introduced by Graham Higman in [5] as an example of group without finite quotients. Still $H(2)$ has a lot of quotients, moreover, it is SQ-universal, [9]. Actually the proof of [9] works for $H(k)$, $k \geq 2$, so, $H(k)$ is SQ-universal for any $k \geq 2$. Some other techniques that were used for $H(2)$ seem to be applicable for $H(k)$, see [4, 8]. But $H(k)$ for $k > 2$ have another, compared with $H(2)$, behavior with respect to finite quotients. Particularly, $H(k)$ has an arbitrary large p -quotient for $p|(k-1)$. Moreover, the intersection of the kernels of these quotient maps intersects trivially with the Baumslag-Solitar subgroups $B(1, k) = \langle a_i, a_{i+1} \rangle < H(k)$. Using [4] it implies the following statement:

¹This work was partially supported by the European Research Council (ERC) grant no. 259527 of G. Arzhantseva, part of this work was done in the Nizhny Nivgorod University and supported by the RSF (Russia) grant 14-41-00044. The stay in Vienna was supported by ERC grant no. 259527 of G. Arzhantseva.

Proposition. *Let $p|(k-1)$ be a prime. Then for any $\varepsilon > 0$ there is an $n \in \mathbb{Z}$ and a bijection $f : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ such that $f(x+1) = kf(x)$ for at least $(1-\varepsilon)p^n$ elements x of $\mathbb{Z}/p^n\mathbb{Z}$ and $f(f(f(f(x)))) = x$ for all $x \in \mathbb{Z}/p^n\mathbb{Z}$.*

The interesting property of this f is that it behaves “almost like” a modular exponent ($x \rightarrow ak^x \pmod{p^n}$), but all its cycles are of the length 4. Precisely, $f(x) = a(x)k^x \pmod{p^n}$ where $a(x) = a(x+1)$ for almost all x ($a(x)$ is “almost a constant”). Maybe, the existence of such functions explains the difficulty in proving estimates for the number of small cycles in repeated modular exponentiation, [2]. The case $k = 2$ is not follows from this notes. So, the existence of f for $k = 2$ is an open question.

Let X be a group (or other algebraic system), $x \in X$ and $\phi : X \rightarrow Y$ be a homomorphism. We systematically, abusing notations, will write x to denote $\phi(x)$ if it is clear from the context that we are dealing with an element of Y . If there are $\phi_j : X \rightarrow Y_j$ we may say “ x of Y_j ” to denote $\phi_j(x)$.

2 p -quotients of a group and its p -central series.

Let G be a group. For $S \subseteq G$ let $\langle S \rangle$ denote the subgroup of G generated by S . For $g, h \in G$ let $[g, h] = g^{-1}h^{-1}gh$ denote the commutator of g and h . For $H_1, H_2 < G$ let $[H_1, H_2] = \langle \{[g, h] \mid g \in H_1, h \in H_2\} \rangle < G$ denote the commutator subgroup of H_1 and H_2 . The p -central series G_1, G_2, \dots of a group G is defined as

$$G_1 = G, \quad G_{i+1} = G_i^p [G_i, G].$$

It is clear by the definition that G/G_{i+1} is the maximal p -quotient of G of p -class at most i . There is another, equivalent, definition of G_k . Let $G_{[i]}$ be the lower central series for G :

$$G_{[1]} = G, \quad G_{[i+1]} = [G_{[i]}, G].$$

Exercise 1. Show that $G_n = \langle G_{[i]}^{p^j}, i+j = n \rangle$. Hint. Using the commutator identities (Theorem 5.1 (Witt-Hall identities) of [7]) show that

$$[u, v^p] = [u, v]^p \cdot [[u, v], v] \cdot [[u, v^2], v] \cdot \dots \cdot [[u, v^{p-1}], v].$$

Particularly, this implies that $[G_{[i]}, G_{[j]}^{p^k}] \subseteq [G_{[i]}, G_{[j]}^{p^{k-1}}]^p [G_{[i+j]}, G_{[j]}^{p^{k-1}}]$. Show that $[G, G_{[i]}^{p^k}] \subseteq \langle G_{[r]}^{p^j}, r+j = i+k+1 \rangle$. Then apply induction on n .

3 Calculating of p -quotients.

Let $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$. Consider the non-commutative ring $\mathbb{Z}_{p^n}[\bar{x}]$ of polynomials with non-commutative (but associative) variables $\bar{x} = (x_0, \dots, x_m)$ over \mathbb{Z}_{p^n} . The ring $\mathbb{Z}_{p^n}[\bar{x}]$ contains finite subring $\mathbb{Z}_{p^n}[p\bar{x}]$ of polynomials $f(p\bar{x})$. It is clear that each

monomial of $f(p\bar{x})$ of order k is divisible by p^k . Inside of $\mathbb{Z}_{p^n}[p\bar{x}]$ there is a group $\Gamma = \langle (1 + px_0), \dots, (1 + px_m) \rangle$, generated by $(1 + px_i)$. Notice, that

$$(1 + px)^{-1} = \sum_{j=0}^{n-1} (-p)^j x^j$$

Lemma 1. $(1 + px_i)^{p^n} = 1$ in $\mathbb{Z}_{p^n}[\bar{x}]$. In other words $j \rightarrow (1 + px_i)^j$ is a function $\mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}[\bar{x}]$.

Lemma 2 (Jacobson). Γ is isomorphic to F/F_n where F is a free group of rank $m + 1$.

We prove this lemma in Section 8. Let I be a (two-sided) ideal in $\mathbb{Z}_{p^n}[\bar{x}]$ and $\phi : \mathbb{Z}_{p^n}[\bar{x}] \rightarrow \mathbb{Z}_{p^n}[\bar{x}]/I$ be a natural map. Let $\Gamma_I = \phi(\Gamma)$. We are going to use Γ_I for calculating G/G_n as follows. Let

$$G = \langle a_0, \dots, a_m \mid u_i(a_0, \dots, a_m) = w_i(a_0, \dots, a_m), i = 0, \dots, k \rangle.$$

Let $g_i = p^{-\alpha_i}(u_i(1 + px_0, \dots, 1 + px_k) - w_i(1 + px_0, \dots, 1 + px_k))$, where p^{α_i} divides all coefficients of $u_i(1 + px_0, \dots, 1 + px_k) - w_i(1 + px_0, \dots, 1 + px_k)$ and being maximal with this property. Consider $I = I(g_i, i = 0, \dots, k)$, an ideal in $\mathbb{Z}_{p^n}[\bar{x}]$ generated by g_i .

Lemma 3. Γ_I is a homomorphic image of G/G_n .

Proof. By construction Γ_I is a homomorphic image of G under $\phi : a_i \rightarrow (1 + px_i)$. It is easy to check that $\phi(G_n) = \{1\}$. \square

When Γ_I is isomorphic to G/G_n ? Probably the answer is the following: if $p \neq 2$ then Γ_I is isomorphic to G/G_n ; for $p = 2$ there are G such that Γ_I is not isomorphic to G/G_n . Probably, it is well known. Otherwise, one may try to use similar technique as in the proof of Lemma 2 (see, Section 8) taking into account the solution of the dimension subgroup problem. See [3] and the bibliography therein for the dimension subgroup problem.

4 p -quotients of $H(k)$, $p \mid (k - 1)$.

$H(k) = \langle a_0, \dots, a_3 \mid \{a_{i+1}a_i = a_i a_{i+1}^k, i = 0, \dots, 3\} \rangle$, here $i + 1$ is taken mod 4. This is a presentation of the Higman group without inversion. Let $p \mid (k - 1)$ then substituting $a_i = (1 + px_i)$ leads

$$g_i = \frac{1}{p^2}(a_{i+1}a_i - a_i a_{i+1}^k) = x_{i+1}x_i - x_i x_{i+1} + Q_0(x_{i+1}) + pQ_1(x_i, x_{i+1}). \quad (1)$$

Our aim is to study $I = I(g_0, g_1, g_2, g_3)$ in $\mathbb{Z}_{p^n}[x_0, \dots, x_3]$, or precisely, $\mathbb{Z}_{p^n}[x_0, \dots, x_3]/I$ and Γ_I . To this end we introduce some notions.

Definition 1. A (non-commutative) ring A is called to be an algebra over \mathbb{Z}_{p^n} if

- A has the unity $1 \in A$.
- Multiplication is \mathbb{Z}_{p^n} -bilinear.

An algebra A is tame if A is a free \mathbb{Z}_{p^n} -modul with a free basis $\mathcal{A} \ni 1$.

All algebras over \mathbb{Z}_{p^n} we deal with are tame. So, in what follows we use just “algebra” to denote “tame algebra”.

Definition 2. Let A (resp. B) be a \mathbb{Z}_{p^n} -algebra and $\mathcal{A} \ni 1$ (resp. $\mathcal{B} \ni 1$) be a set of it's free generators as a \mathbb{Z}_{p^n} -modul. A Zappa-Szep product $C = A \bowtie B$ is a \mathbb{Z}_{p^n} algebra such that

- C contains isomorphic copies of A and B such that $A \cap B = \mathbb{Z}_{p^n} \cdot 1$ (we have fixed such a copies of A and B and denote them by the same letters).
- The set $\{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\}$, as well as the set $\{ba \mid a \in \mathcal{A}, b \in \mathcal{B}\}$, forms a free basis of C as a \mathbb{Z}_{p^n} -modul.

Exercise 2. It looks that by definition one should say that $C = A \bowtie B$ with respect to \mathcal{A} and \mathcal{B} . Show that $C = A \bowtie B$ with respect to any free bases $\mathcal{A}' \ni 1$ and $\mathcal{B}' \ni 1$.

Definition 3. Let K, L be a groups. A Zappa-Szep product $G = K \bowtie L$ of groups K and L is a group such that

- G contains isomorphic copies of K and L . We fix such copies and assume that $K, L < G$.
- $K \cap L = \{1\}$ in G .
- $G = KL$. (This easily implies that $G = LK$.)

Remark. Of course, the definitions do not imply that a Zappa-Szep product is uniquely defined by a pair of algebras o groups. Really, in order to define $X \bowtie Y$ uniquely (up to isomorphism) one needs a function $com : X \times Y \rightarrow Y \times X$ which describe how the elements of X commute with elements of Y . So, in some sense, $Z = X \bowtie Y$ is an abuse of notation. In any case, when we use $Z = X \bowtie Y$, the structure of Z will be described.

Theorem 1. Let $I = I(g_0, g_1, g_2, g_3)$ be an ideal in $\mathbb{Z}_{p^n}[\bar{x}]$ generated by g_i of Eq.(1). Then $\mathbb{Z}_{p^n}[\bar{x}]/I = \mathbb{Z}_{p^n}[x_0, x_2] \bowtie \mathbb{Z}_{p^n}[x_1, x_3]$.

Recall, that G_i denotes the i -th term of the p -central series of group $G = G_0$. Also we suppose that $p \mid (k - 1)$.

Corollary 1. There is a surjective homomorphism $H(k)/H_n(k) \rightarrow F/F_n \bowtie F/F_n$, where F is a free group of rank 2.

Proof. By Lemma 3 $H(k)/H_n(k)$ surjects into Γ_I . By Theorem 1 and Lemma 2 there are $S, \tilde{S} < \Gamma_I$ such that

- $S = \langle a_0 = (1 + px_0), a_2 = (1 + px_2) \rangle, \tilde{S} = \langle a_1 = (1 + px_1), a_3 = (1 + px_3) \rangle;$
- S and \tilde{S} are isomorphic to F/F_n ;
- $S \cap \tilde{S} = \{1\};$

It follows that $|S\tilde{S}| = |S| \cdot |\tilde{S}|$ and $S\tilde{S} \leq \Gamma_I$. So, we have to prove that $\Gamma_I \subset S\tilde{S}$. To this end it suffices to show that in Γ_I there exist relations removing appearance of $a_1^m a_0^r, a_1^m a_2^r, a_3^m a_0^r$ and $a_3^m a_2^r$. By Lemma 1 we may assume that $m, r \in \mathbb{Z}_{p^n}$. The relation $a_1 a_0 = a_0 a_1^k$ implies $a_1^m a_0^r = a_0^r a_1^{mk^r}$. The relation $a_2 a_1 = a_1 a_2^k$ implies $a_1^m a_2^r = a_2^{rk^{-m}} a_1^m$. Considerations for the other indexes are the same. Notice here, that the condition $p|(k-1)$ implies that $r \rightarrow k^r$ is a well definite function $\mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$. \square

5 What is going on

Consider $w \in H_k$ as a word $a_{i_1}^{n_1} a_{i_2}^{n_2} \dots$ but now suppose that n_j are in some commutative ring, in our example, $n_j \in \mathbb{Z}_{p^n}$. We get a new group \tilde{H}_k which is a homomorphic image of H_k . Now, the relation $a_1^k = a_0^{-1} a_1 a_0$ implies as well the relation $a_1^{1/k} = a_0 a_1 a_0^{-1}$. We also need that $j \rightarrow k^j$ is well defined mod p^n . After that any element of \tilde{H}_k may be written as wu , where $w = a_0^{n_1} a_2^{m_1} \dots a_2^{m_j}, n_i, m_i \in \mathbb{Z}_{p^n}$ and, similarly, $u = u(a_1, a_3)$. So, we have $\tilde{H}_k = (\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n}) \rtimes (\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n})$. The whole problem is to show that the natural homomorphism $\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n} \rightarrow F/F_n$ is compatible with the \rtimes structure. (Here F is a rank 2 free group). Which, probably, may be done another way as well...

Let restate all it more formally. One can easily check that if $G_1 = H_1 \rtimes K$ and $G_2 = H_2 \rtimes K$ then $G_1 \underset{K=K}{*} G_2 = (H_1 * H_2) \rtimes K$. For $H_k, p|(k-1)$ we have the following:

- $BS(1, k) \rightarrow BS_{p^n}(1, k) = \mathbb{Z}_{p^n} \rtimes_k \mathbb{Z}_{p^n},$
- $B_3 \rightarrow BS_{p^n} \underset{\mathbb{Z}_{p^n}}{*} BS_{p^n} = (\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n}) \rtimes \mathbb{Z}_{p^n},$ where we amalgamate the different factors of BS_{p^n} .
- Finally we get $H_k \rightarrow (\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n}) \rtimes (\mathbb{Z}_{p^n} * \mathbb{Z}_{p^n}).$

For the case $k = 2$ we may do similar things. We need a unitary commutative ring R such that function $r \rightarrow 2^r$ is defined in R . Such a ring exists, for example the real numbers \mathbb{R} . So, we may embed $BS(1, 2) \hookrightarrow \mathbb{R} \rtimes_2 \mathbb{R}$, where for $(\alpha_i, \beta_i) \in \mathbb{R} \rtimes_2 \mathbb{R}$ the multiplication is defined as $(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, 2^{\alpha_2} \beta_1 + \beta_2)$. Similarly, there is a homomorphism $B_3 \rightarrow (\mathbb{R} * \mathbb{R}) \rtimes \mathbb{R}$, which is not injective, but nontrivial. And finally we obtain $H_2 \rightarrow H_{\mathbb{R}} = (\mathbb{R} * \mathbb{R}) \rtimes (\mathbb{R} * \mathbb{R})$. (Any element of $(\mathbb{R} * \mathbb{R}) \rtimes (\mathbb{R} * \mathbb{R})$ is of the form $wu, w = a_0^{\alpha_1} a_2^{\beta_1} \dots a_2^{\beta_k}, \alpha_i \beta_i \in \mathbb{R}$ and, similarly, $u = u(a_1, a_3)$.) Actually, H_k has a nontrivial homomorphic image in $H_{\mathbb{R}}$ for any $k \in \mathbb{Z}$.

What is the structure of $H_{\mathbb{R}}$? Changing $a_i \rightarrow a_i^\delta$ we may write

$$H_{\mathbb{R}} = \langle a_i^\alpha, i = 0, \dots, 3, \alpha \in \mathbb{R} \mid a_i^{-\alpha} a_{i+1}^\beta a_i^\alpha = a_{i+1}^{\beta \exp(\alpha)} \rangle.$$

It is not hard to show that $\langle a_0^\alpha, a_1^\alpha, a_2^\alpha, a_3^\alpha \rangle < H_{\mathbb{R}}$ is residually finite for all $\alpha \notin Y$ for a countable set $Y \subset \mathbb{R}$.

6 Proof Theorem 1

The algebra $\mathbb{Z}_{p^n}[\bar{x}]/I$ may be constructed as amalgamated free products, similar to the construction of the Higman group itself.

Definition 4. Let A, B be \mathbb{Z}_{p^n} -algebras, $\mathcal{A} \ni 1, \mathcal{B} \ni 1$ their corresponding free generators as \mathbb{Z}_{p^n} -modules. A free product $A * B$ is a \mathbb{Z}_{p^n} -algebra that

- Generated by 1 and alternating words of letters from $\mathcal{A}' = \mathcal{A} \setminus \{1\}$ and $\mathcal{B}' = \mathcal{B} \setminus \{1\}$ as a free \mathbb{Z}_{p^n} -module. A word $w = w_1 w_2 \dots w_r$ is alternating if $(w_i, w_{i+1}) \in \mathcal{A}' \times \mathcal{B}' \cup \mathcal{B}' \times \mathcal{A}'$.
- It suffices to define product for two alternating words $w = w_1 \dots w_r$ and $u = u_1 \dots u_k$. So, $wu = w_1 \dots w_r u_1 \dots u_k$ if (w_r, u_1) alternating and $wu = w_1 \dots w_{r-1} (w_r \cdot u_1) u_2 \dots u_k$ otherwise. Here $w_r \cdot u_1$ is the product in A or B .

For example, $\mathbb{Z}_{p^n}[x] * \mathbb{Z}_{p^n}[x] = \mathbb{Z}_{p^n}[x_0, x_1]$.

Exercise 3. Check that $A * B$ is well defined, independent of \mathcal{A} and \mathcal{B} , contains isomorphic copies of A and B with intersection equals to $\mathbb{Z}_{p^n} \cdot 1$ and satisfies the universal property of free product of algebras.

Definition 5. Let $C_1 = A \bowtie V$ and $C_2 = B \bowtie V$. We define $C = C_1 \underset{V}{*} C_2$ as $C = (A * B) \bowtie V$. Let \mathcal{A}, \mathcal{B} and \mathcal{V} be free bases of A, B , and V , correspondingly. Any element is a \mathbb{Z}_{p^n} -combination of wv , where w is alternating word of letters from $\mathcal{A}', \mathcal{B}'$ and $v \in \mathcal{V}$. In order to define multiplication on C it suffices to define vw as a combination of $w_i v_i$. It could be done using Zappa-Zsep product structure of C_1 and C_2 . Suppose, for example that $w = a_1 b_1 \dots a_k b_k$ then

$$\begin{aligned} v a_1 b_1 \dots a_k b_k &= \sum_{i_1} a_{i_1}^1 v_{i_1} b_1 \dots a_k b_k = \sum_{i_1, j_1} a_{i_1}^1 b_{i_1, j_1}^1 v_{i_1, j_1} \dots a_k b_k = \\ &= \sum_{i_1, j_1, \dots, i_k, j_k} a_{i_1}^1 b_{i_1, j_1}^1 \dots a_{i_k}^k b_{i_k, j_k}^k v_{i_1, j_1, \dots, i_k, j_k} \end{aligned}$$

Exercise 4. Check that $C_1 \underset{V}{*} C_2$ is well defined, contains isomorphic copies of C_1 and C_2 such that $C_1 \cap C_2 = V$. Check that $C_1 \underset{V}{*} C_2$ satisfies the universal property of amalgamated free products of algebras.

Consider $A_0 = \mathbb{Z}_{p^n}[x_0, x_1]/I(g_0)$, where $I(g_0)$ is the ideal generated by g_0 of Eq.(1).

Proposition 1. $A_0 = \mathbb{Z}_{p^n}[x_0] \bowtie \mathbb{Z}_{p^n}[x_1]$

We prove the proposition in Section 7. Now let us show how Theorem 1 follows from Proposition 1. Let $A_1 = \mathbb{Z}[x_1, x_2]/I(g_1)$. Clearly, A_1 is isomorphic to A_0 , so $A_1 = \mathbb{Z}_{p^n}[x_1] \bowtie \mathbb{Z}_{p^n}[x_2]$. Consider $A_{01} = A_0 *_{\mathbb{Z}_{p^n}[x_1]} A_1$. Notice, that the roles of $\mathbb{Z}_{p^n}[x_1]$ in A_0 and A_1 are different, precisely the isomorphism from A_0 to A_1 maps $\mathbb{Z}_{p^n}[x_1]$ to $\mathbb{Z}_{p^n}[x_2]$ not to $\mathbb{Z}_{p^n}[x_1]$ of A_1 .

Lemma 4. $A_{01} = \mathbb{Z}_{p^n}[x_0, x_2] \bowtie \mathbb{Z}_{p^n}[x_1]$ is isomorphic to $\mathbb{Z}_{p^n}[x_0, x_1, x_2]/I(g_0, g_1)$.

Proof. By construction $g_0 = g_1 = 0$ in A_{01} . So, the map $x_i \rightarrow x_i$ prolongs to a surjective homomorphism $\phi : \mathbb{Z}_{p^n}[x_0, x_1, x_2]/I(g_0, g_1) \rightarrow A_{01}$. Using the universal property of A_{01} define $\psi : A_{01} \rightarrow \mathbb{Z}_{p^n}[x_0, x_1, x_2]/I(g_0, g_1)$. Notice, that ψ is surjective as well ($\mathbb{Z}_{p^n}[x_0, x_1, x_2]/I(g_0, g_1)$ is generated by x_i). Check that $\psi\phi = id : A_{01} \rightarrow A_{01}$ by the universal property. \square

Similarly, the algebras $A_2 = \mathbb{Z}_{p^n}[x_2, x_3]/I(g_2)$, $A_3 = \mathbb{Z}_{p^n}[x_3, x_0]/I(g_3)$, and $A_{23} = A_2 *_{\mathbb{Z}_{p^n}[x_3]} A_3 = \mathbb{Z}[x_2, x_0] \bowtie \mathbb{Z}[x_3]$ may be constructed. Notice, that there exist isomorphism $A_{01} \rightarrow A_{23}$ that sends $x_0 \rightarrow x_2$, $x_2 \rightarrow x_0$, $x_1 \rightarrow x_3$. Now, we may construct $A = A_{01} *_{\mathbb{Z}_{p^n}[x_0, x_2]} A_{23}$ (we make isomorphism $\mathbb{Z}[x_0, x_2]$ of A_{01} with $\mathbb{Z}[x_2, x_0]$ of A_{23} sending $x_0 \rightarrow x_0$ and $x_2 \rightarrow x_2$). Theorem 1 follows from the lemma.

Lemma 5. $A = \mathbb{Z}_{p^n}[x_0, x_2] \bowtie \mathbb{Z}_{p^n}[x_1, x_3]$ is isomorphic to $\mathbb{Z}_{p^n}[x_0, x_1, x_2, x_3]/I(g_0, \dots, g_3)$.

7 Proof of Proposition 1

The proof is based on the fact that a polynomial g_0 forms a kind of a Grobner basis (over non-commutative polynomials). We will not define what a Grobner basis is for non-commutative polynomials. Instead, we directly apply a Knuth-Bendix algorithm [1] to $\{g_0\}$.

Let $m(y_1, \dots, y_k)$ be a non-commutative monomial or, the same, a word in alphabet $\{y_1, \dots, y_k\}$, that is, $m(y_1, \dots, y_k) = z_1 z_2 \dots z_r$, $z_i \in \{y_1, \dots, y_k\}$. The product of two monomials is just the concatenation. A non-commutative polynomial f over \mathbb{Z}_{p^n} is a “linear” combination of monomials $f = \sum a_i m_i$, $a_i \in \mathbb{Z}_{p^n}$. The product $f_1 f_2$ of polynomials is defined using the product of monomials by linearity.

Let us return to the study of $A_0 = \mathbb{Z}_{p^n}[x_0, x_1]/I(g_0)$. We call a polynomial $f \in \mathbb{Z}_{p^n}[x_0, x_1]$ left (resp. right) reduced if $f = \sum a_{i,j} x_0^i x_1^j$ (resp. $f = \sum a'_{i,j} x_1^i x_0^j$). Proposition 1 is equivalent to the claim.

Claim 1. For any $f \in \mathbb{Z}_{p^n}[x_0, x_1]$ there exists a left (resp. right) reduced polynomial \tilde{f} such that $f - \tilde{f} \in I$. If $f \in I$ is left (right) reduced then $f = 0$.

From this point we restrict ourselves to the left case. The right case may be considered similarly. Define the one step reduction based on equalities $g_0 = 0$:

$$x_1 x_0 \xrightarrow{\rho} x_0 x_1 - Q_0(x_1) - p Q_1(x_0, x_1)$$

Let $f, \tilde{f} \in \mathbb{Z}_{p^n}[x_0, x_1]$.

- \tilde{f} is a one step reduction of f ($f \xrightarrow{\rho} \tilde{f}$) if an appearance of x_1x_0 , in some monomial of f is changed according to the above described rule; \tilde{f} is the resulting polynomial (after applying associativity and linearity).
- f is said to be terminal if no monomial of f contains x_1x_0 . It means that we are unable to apply $\xrightarrow{\rho}$ to f .
- We write $f \xRightarrow{\rho} \tilde{f}$ (\tilde{f} is a reduction of f) if there is a sequence $f_0 = f, f_1, \dots, f_k = \tilde{f}$ such that $f_i \xrightarrow{\rho} f_{i+1}$ for $i = 0, \dots, k-1$.
- We write $f \xRightarrow{\rho} \tilde{f}+$ if $f \xRightarrow{\rho} \tilde{f}$ and \tilde{f} is terminal.

Proposition 2. • f is terminal if and only if f is left reduced.

- There is no infinite sequence $f_0 \xrightarrow{\rho} f_1 \xrightarrow{\rho} f_2 \dots$
- For any non-terminal f there exist a unique \tilde{f} such that $f \xRightarrow{\rho} \tilde{f}+$.

Two last items mean that any sequence $f \xrightarrow{\rho} f_1 \xrightarrow{\rho} \dots$ of one step reduction terminates and the terminal polynomial depends only on f .

We prove the proposition in Subsection 7.1. Now let us show how Proposition 2 implies Claim 1. We use notation $f = \xrightarrow{\rho} f'$ (resp. $f = \xRightarrow{\rho} f'$) to denote $f \xrightarrow{\rho} f'$ or $f = f'$ (resp. $f \xRightarrow{\rho} f'$ or $f = f'$).

Lemma 6. The map $f = \xRightarrow{\rho} \tilde{f}+$ is linear, that is, if $f_1 = \xRightarrow{\rho} \tilde{f}_1+$ and $f_2 = \xRightarrow{\rho} \tilde{f}_2+$ then $a_1f_1 + a_2f_2 = \xRightarrow{\rho} a_1\tilde{f}_1 + a_2\tilde{f}_2$, where $a_1, a_2 \in \mathbb{Z}_{p^n}$.

Proof. Let $a_1f_1 + a_2f_2 \xrightarrow{\rho} f'$. It means that we apply reduction to a monomial m of $a_1f_1 + a_2f_2$. The monomial m may appear in f_1 , f_2 , or in the both polynomials. In any case there exist f'_1 and f'_2 such that $f_1 = \xrightarrow{\rho} f'_1$, $f_2 = \xrightarrow{\rho} f'_2$ and $f' = a_1f'_1 + a_2f'_2$. It follows by induction that if $a_1f_1 + a_2f_2 \xRightarrow{\rho} f'$ then $f' = a_1f'_1 + a_2f'_2$ for some f'_1, f'_2 such that $f_1 = \xRightarrow{\rho} f'_1$ and $f_2 = \xRightarrow{\rho} f'_2$. Now suppose that $a_1f'_1 + a_2f'_2$ is terminal but, say, f'_1 is not terminal. There are two possibilities:

1. $a_1f'_1$ is terminal. In this case, collecting terminal monomials, we may write $f'_1 = \alpha + \beta$ with α terminal and $a_1\beta = 0$. In this case further reduction of f'_1 does not change $a_1f'_1$. So, w.l.g. we may assume f'_1 to be terminal.
2. $a_1f'_1$ is not terminal. In this case we may write $f'_i = \alpha_i + \beta_i$ with α_i terminal and $a_1\beta_1 + a_2\beta_2 = 0$. Now, apply the same reduction to β_1 and β_2 , keeping the sum $a_1f'_1 + a_2f'_2$ unchanged.

We are done by Proposition 2. □

Lemma 7. $f \xRightarrow{\rho} 0+$ if and only if $f \in I(g_0, \dots, g_3)$.

Proof. Only if. It is clear by construction that $f \xRightarrow{\rho} \tilde{f}$ implies that $f - \tilde{f} \in I$.

If. Let $f \in I$. It means that $f = \sum \alpha_i g_0 \beta_i$. Applying associativity we may write $f = \sum a_i m_i g_0 m'_i$, where m_i and m'_i are monomials and $a_i \in \mathbb{Z}_{p^n}$. By construction, there is a one step reduction $m_i g_0 m'_i \xrightarrow{\rho} 0$. We are done by Lemma 6 and Proposition 2. □

7.1 Proof of Proposition 2.

The first item of Proposition 2 is straightforward. So we start with the proof of the second item of the proposition. It is the most difficult part of the proposition and will be used for the proof of the third item.

7.1.1 Proof of the second item.

Let $t = a_j m(x_0, x_1)$ be a term (a monomial with a coefficient). We are going to measure how an application of one step reduction makes a term more close to a left reduced polynomial. To this end we define:

- $|t| = \min\{k \in \mathbb{N} \mid p^k t = 0\}$.
- $n_0(t)$ – number of x_0 in t , for example, $n_0(x_1^i x_0^j) = j$.
- $def(t)$ – the defect of t , the total number of pairs where x_1 appears before x_0 , for example, $def(x_1^j x_0^k x_1^r x_0^m) = jk + jm + rm$.

To each term we associate the ordered triple $(|t|, n_0(t), def(t))$. On the set of triple we consider lexicographical order: $(\alpha, \beta, \gamma) < (\alpha', \beta', \gamma')$ iff

- $\alpha < \alpha'$; or
- $\alpha = \alpha'$ and $\beta < \beta'$; or
- $\alpha = \alpha'$, $\beta = \beta'$, and $\gamma < \gamma'$.

Now one may check that $(|t|, n_0(t), def(t)) > (|t_j|, n_0(t_j), def(t_j))$ if $t \xRightarrow{p} \sum_j t_j$. We need the following result.

Lemma 8 (Dickson). *Any decreasing (with respect to lexicographic order) sequences in \mathbb{N}^3 is finite.*

Consider now the reduction process of t as a tree: To each vertex we associate a term in such a way that in any reduction step the resulting polynomial is a sum of terms of the leafs of the tree. With root we associate t . For each reduction of term t' in a leaf l we connect the leaf l with new leafs with all terms appearing in the reduction. Any descending path in this tree is finite by Dickson Lemma. This tree is k -regular by construction, so the tree is finite and the reduction process terminates.

7.1.2 Proof of the third item.

This uses the Newman's lemma, or Diamond lemma for reduction processes.

Suppose that on a set X a reduction process $\cdot \xrightarrow{*} \cdot$ (just a relation on X) is defined. Denote by $\xRightarrow{*}$ it's transitive closure. We say that x is terminal if there are no $y \in X$ such that $x \xRightarrow{*} y$. As before, let $x \xRightarrow{*} y$ denotes $x \xrightarrow{*} y$ and y is terminal.

Lemma 9 (Diamond lemma). *Let $\xrightarrow{*}$ satisfies the following properties:*

- Any sequence $x_1 \xrightarrow{*} x_2 \xrightarrow{*} \dots$ is finite.
- $\xrightarrow{*}$ is locally confluent, that is, for any x, y_1 and y_2 such that $x \xrightarrow{*} y_1$ and $x \xrightarrow{*} y_2$ there exists $z \in X$ such that $y_1 \xRightarrow{*} z$ and $y_2 \xRightarrow{*} z$.

Then $\xRightarrow{*}$ is globally confluent, that is, for any non-terminal x there exists unique y such that $x \xRightarrow{*} y$.

So, in order to show Proposition 1 it suffices to check the second condition of the Diamond Lemma for $\xrightarrow{\rho}$. Let $f \xrightarrow{\rho} f_1$ and $f \xrightarrow{\rho} f_2$. If the reduction applies to a different terms then existence of f_3 , $f_1 \xrightarrow{\rho} f_3$ and $f_2 \xrightarrow{\rho} f_3$ is trivial. It suffices to consider $f = ax_{i_1} \dots x_{i_m}$. Suppose w.l.g., that $f \xrightarrow{\rho} f_1$ is an application of reduction to $x_{i_j} x_{i_{j+1}} = x_1 x_0$ and $f \xrightarrow{\rho} f_2$ $x_{i_k} x_{i_{k+1}} = x_1 x_0$ for $k > j + 1$. Then $f_1 = ax_{i_1} \dots x_{i_{j-1}} q x_{i_{j+2}} \dots x_{i_m}$ and $f_2 = ax_{i_1} \dots x_{i_{k-1}} q x_{i_{k+2}} \dots x_{i_m}$, where $q = x_0 x_1 - Q_0(x_1) - p Q_1(x_0, x_1)$. One may check that $f_1 \xRightarrow{\rho} f_3$ and $f_2 \xRightarrow{\rho} f_3$ for $f_3 = ax_{i_1} \dots x_{i_{j-1}} q x_{i_{j+2}} \dots x_{i_{k-1}} q x_{i_{k+2}} \dots x_{i_m}$.

8 Proof of Lemma 2

Let $\mathbb{Z}(\bar{x})$ be an algebra of power series with noncommutative (but associative) variables $\bar{x} = x_0, x_1, \dots, x_m$ over \mathbb{Z} . For $a, b \in \mathbb{Z}(\bar{x})$ let $[a, b] = ab - ba$ and $\Lambda[\bar{x}]$ be a submodule of $\mathbb{Z}[\bar{x}]$ generated by $[\cdot, \cdot]$ starting from \bar{x} . Let $\Lambda^j \subset \Lambda[\bar{x}]$ consist of uniform polynomials of order j . So,

$$\Lambda[\bar{x}] = \bigcup_{j=0}^{\infty} \Lambda^j.$$

Let $I = I(\bar{x})$ be a (two-sided) ideal in $\mathbb{Z}(\bar{x})$ generated by \bar{x} . Clearly, this ideal consists of polynomials without constant term. Let G be a group. Notations G_n and $G_{[n]}$ are defined in Section 2.

Theorem 2 (Magnus' theorem). • Let $a_i = 1 + x_i$. The group $F = \langle a_i \rangle$ is a free group, freely generated by a_i .

- $(1 + I^n) \cap F = F_{[n]}$.
- If $w \in F_{[n]}$ then $w = 1 + d + z$, where $d \in \Lambda^n$ and z does not contain terms of order $\leq n$.
- For any $d \in \Lambda^n$ there exists $z \in \mathbb{Z}[\bar{x}]$ without terms of order $\leq n$ such that $1 + d + z \in F_{[n]}$.

Consider homomorphism $\pi : \mathbb{Z}(\bar{x}) \rightarrow \mathbb{Z}(\bar{x})$, defined by $\pi(x_i) = p x_i$. Clearly, $\pi(\mathbb{Z}(\bar{x})) = \mathbb{Z}(p\bar{x})$. Also, $\pi(F)$ is an inclusion of a free group F into $\mathbb{Z}(p\bar{x})$. For a two sided ideal J of $\mathbb{Z}(p\bar{x})$ let $N_j = \{w \in \pi(F) \mid w - 1 \in J\}$.

Lemma 10. $N_j \triangleleft \pi(F)$.

Clearly, $\mathbb{Z}(\bar{x})/p^n\mathbb{Z}(\bar{x}) \equiv \mathbb{Z}_{p^n}(\bar{x})$. Denote $(p^n) = p^n\mathbb{Z}(\bar{x}) \cap \mathbb{Z}(\bar{p}x)$. Notice, that $\mathbb{Z}_{p^n}(p\bar{x}) = \mathbb{Z}_{p^n}[p\bar{x}]$. Now, Lemma 2 is a consequence of the following theorem.

Theorem 3 (Jacobson, [6]). $N_{(p^n)} = \pi(F_n)$

Proof. We present here the Jacobson proof (see [6]) which is a reduction to Theorem 2. In [6] the definition of (p^n) is different and not equivalent of ours. But the proof in [6] is, actually, for our definition of (p^n) .

Notice, that $(1 + p^m w \dots)^p = 1 + p^{m+1} \dots$ and $[(1 + p^m w \dots), (1 + p^k u \dots)] = 1 + p^{m+k}(wu - uw) \dots$ where the omitted terms are of higher p -order. This implies that $N_{(p^m)}^p \subseteq N_{(p^{m+1})}$ and $[N_{(p^m)}, N_{(p^k)}] \subseteq N_{(p^{m+1})}$. Consequently, we have $\pi(F_n) \subseteq N_{(p^n)}$ and $N_{(p^{n+1})} \subseteq N_{(p^n)}$.

According to [6] we show the equality $N_{(p^n)} = \pi(F_n)$ by induction. By definition, $N_{(p^1)} = \pi(F_1) = \pi(F)$. Suppose, that $N_{(p^n)} = \pi(F_n)$. Then we know that $\pi(F_{n+1}) \subseteq N_{(p^{n+1})} \subseteq \pi(F_n)$. So, it suffices to show that $\pi(F_n) \cap \pi(F_{n+1}) \supseteq N_{(p^{n+1})} \cap \pi(F_n)$, or, the same, to prove that if $w \in \pi(F_n) \setminus \pi(F_{n+1})$ then $w \notin N_{(p^{n+1})}$. Let $w \in \pi(F_n) \setminus \pi(F_{n+1})$. There exists a unique i such that $w \in \pi(F_{[i]}) \setminus \pi(F_{[i+1]})$. By Theorem 2 $w = 1 + p^j d_i(p\bar{x}) + z$ where $d_i \in \Lambda^i$, z has \bar{x} -order more than i . Also we have that $i + j \geq n$ (as $w \in N_{(p^n)}$). Applying once again Theorem 2 we find $u = 1 + d_i(p\bar{x}) + z' \in \pi(F_{[i]})$, where the \bar{x} -order of z' is more than i . So, $w = u^{p^j} w_1$, where $w_1 \in \pi(F_{[i']})$ for $i' > i$. Repeating this procedure one gets $w = u_1^{p^{j_1}} u_2^{p^{j_2}} \dots u_k^{p^{j_k}} w_k$, where $w_k \in \pi(F_{[n+1]})$ and $u_r = (1 + d_{i_r}(p\bar{x}) \dots)$ with $d_{i_r} \in \Lambda^{i_r}$ (term of higher order in \bar{x} are omitted) and $i_r + j_r \geq n$. Now, $u_r \in \pi(F_{[i_r]})$ and, consequently, $u_r^{p^{j_r}} \in \pi(F_{[i_r]})^{p^{j_r}} \subseteq F_{[i_r + j_r]}$. If $\forall r \ i_r + j_r > n$ then $w \in \pi(F_{n+1})$, so, by our assumptions, $i_r + j_r = n$ for some r . It implies that $w = u_1^{p^{j_1}} \dots u_k^{p^{j_k}} w_k = (1 + p^{j_1} d_{i_1}(p\bar{x}) + p^{j_2} d_{i_2}(p\bar{x}) \dots) \notin N_{(p^{n+1})}$. \square

Let $F = \langle a_0, \dots, a_m \rangle$ be a free group on $\{a_0, \dots, a_m\}$. Let $\mathbb{Z}_{p^n}[F/F_n]$ be a group algebra of F/F_n over \mathbb{Z}_{p^n} . Theorem 3 implies that there exists unique homomorphism $\phi : \mathbb{Z}_{p^n}[F/F_n] \rightarrow \mathbb{Z}_{p^n}[p\bar{x}]$ such that $\phi(a_i) = 1 + p x_i$. (Here we, abusing notation, denote by the same symbol a_i its image in F/F_n .) Moreover, $(\ker(\phi) + 1) \cap F/F_n = \{1\}$. Still $\ker(\phi)$ is not trivial. For example, if $w \in F/F_n$ and $w^{p^j} = 1$ then $p^j(w - 1) \in \ker(\phi)$. What is the structure of $\ker(\phi)$? For example, is it true that $\ker(\phi)$ is generated by $\{p^j(w - 1) \mid w \in F/F_n, w^{p^j} = 1\}$?

References

- [1] Franz Baader, Tobias Nipkov. *Term Rewriting and All That*, Cambridge University Press 1998. xii+301 pp. ISBN: 0-521-45520-0; 0-521-77920-0 .
- [2] Lev Glebsky and Igor E. Shparlinski. Short cycles in repeated exponentiation modulo a prime. *Des. Codes Cryptogr.*, 56(1):3542, 2010.
- [3] Gupta, N. Lectures on Dimension Subgroups. *Resenhas IME-USP*, 1996, Vol.2, No.3, 263-273

- [4] Harald A. Helfgott and Kate Juschenko. Soficity, short cycles and the Higman group. *Preprint* arXiv:1512.02135
- [5] Graham Higman. A finitely generated infinite simple group. *J. London Math. Soc.*, 26:6164, 1951.
- [6] Jacobson, N.(1-YALE) Magnus' method in the theory of free groups. *Ulam Quart.* 1 (1992), no. 1,
- [7] Magnus, Wilhelm; Karrass, Abraham; Solitar, Donald *Combinatorial group theory. Presentations of groups in terms of generators and relations.* Dover Publications, Inc., Mineola, NY, 2004. xii+444 pp. ISBN: 0-486-43830-9 Reprint of the 1976 second edition.
- [8] Alexandre Martin, On the cubical geometry of Higman's group. *Preprint* arXiv:1506.02837
- [9] Schupp, Paul E. Small cancellation theory over free products with amalgamation. *Math. Ann.* 193 (1971), 255264